

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

Remarks

The present amendment responds to the Official Action dated February 26, 2004. The Official Action objected to Figs. 1 and 4 as not being labeled "Prior Art." The Official Action also objected to Figs. 1 and 4 on the grounds that certain elements needed labels. The Official Action rejected claims 1, 5, and 10 under 35 U.S.C. §102(b) based on Little et al. PCT Publication No. WO 97/04395 (Little). Claim 2 was rejected under 35 U.S.C. 103(a) based on Little in view of Chaum U.S. Patent No. 4,529,870 (Chaum). Claim 3 was rejected under 35 U.S.C. 103(a) based on Little in view of McNair U.S. Patent No. 5,278,905 (McNair). Claims 4, 6-9, and 11 were rejected under 35 U.S.C. 103(a) based on Little in view of Schneier, *Applied Cryptography Second Edition: protocols, algorithms, and source code in C*, 1996 (Schneier). These grounds of rejection are addressed below following a brief discussion of the present invention to provide context.

Claims 1, 3, 5, and 10 have been amended to be more clear and distinct. Claims 12-20 have been added. Claims 1-20 are presently pending.

The Present Invention

Personal digital assistants (PDAs) are used for storing personal information and for transferring stored personal information between computer systems. It is also possible to use a PDA to prepare and store highly confidential personal information such as transaction information for execution at a self-service terminal (SST) such as an automated teller machine (ATM).

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

However, to provide some security for the transaction information it would be desirable to encrypt the transaction information that is stored on and transmitted from the PDA. A conventional PDA is not an inherently secure device since it has minimal tamper resistance. Minimal tamper resistance means that there is no secure area for storing a secret cryptographic key such as a separately housed encryption device adapted to the PDA. The lack of secure storage limits the use of industry-standard cryptographic techniques with a conventional PDA.

The present invention does not require a secure device for providing encryption keys. Rather, the present invention utilizes an encryption program stored in memory to generate keys for the portable terminal. A financial transaction may be initiated by the portable terminal. The encryption program determines an encryption key based on variable properties of the portable terminal. For example, a variable property would include reading contents of memory which are changed based on the usage history of the portable terminal. See the present application at page 2, lines 14-19. The portable terminal encrypts financial information associated with the financial transaction and communicates the encrypted financial information to an ATM or other suitable self service terminal.

Examiner Interview

The Examiner is thanked for the courtesy of a telephone interview concerning the above case on May 13, 2004. In this call, the Examiner clarified his request for text labels in regard to Figs. 1 and 4. Applicant agreed to amend Figs. 1 and 4 according to the Examiner's request. Applicant explained that labels for lead lines 10 in Fig. 1 and 50 in Fig. 4 would not contain a textual label in the figures and agreed to explain the reason in this response.

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

Drawing Objections

Applicant respectfully disagrees that Figs. 1 and 4 should be labeled prior art. Referring to storage area 28 of Figs. 1 and 2, the contents of the storage area 28 contain instructions in accordance with the present invention. These contents are more fully described in connection with the discussion of Fig. 2. Fig. 2 illustrates an expanded view of the contents of storage area 28. Referring to Fig. 2 and page 7, lines 14-25 of the present specification, storage area 28 includes an encryption program 34, ATM program 32, and account data 30. In one aspect, the encryption program 34, a "means for generating a new key for the prepared financial transaction" as claimed in claim 1, reads the contents of the dynamic heap 26 shown in Fig. 1 to obtain a seed for generating an encryption key. See page 8, lines 23-27 of the present specification. Since the expanded view of Fig. 1 shown in Fig. 2 contains an element of the present invention, Fig. 1 should not be labeled prior art. At page 8, line 12, the transaction system illustrated in Fig. 4 includes PDA 10. PDA 10 also includes the storage area 28 containing the encryption program 34. A proposed amendment to Fig. 4 has been made to make explicit what is already implicit in the drawings by including the encryption program 34. Therefore, Fig. 4 also should not be labeled prior art.

Proposed amendments to Figs. 1 and 4 are submitted herewith. Per the Examiner's request, these amendments add textual labels for elements 16, 26, and 28 of Fig. 1 and elements 10, 52, 54, 56, and 58 in Fig. 4. Numerals 10 (Fig. 1) and 50 (Fig. 4) do not have text labels since these callouts are for the subject matter of the figures as a whole.

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

Amendments to the Specification

The paragraph beginning at page 6, line 17 has been amended to clarify what is clear from the specification as a whole that the PDA depicted in Fig. 1 represents a generic PDA which has been modified in accordance with the teachings of the present invention. Palm IIIx is one example of a PDA which may be suitably modified in accordance with the teachings of present invention.

The paragraph beginning at page 7, line 7 has been amended to clarify what was already clear from the specification as a whole that the contents of storage area 28 are in accordance with the present invention.

Section 112, 1st Paragraph Rejection

Claim 1 was rejected as improperly comprising a single means claim. Claim 1 has been amended to replace the single means clause with a display, an input, a means for generating a new key, and a means for encrypting the financial data with the new key. Thus, this rejection has been addressed and overcome.

The Art Rejections

All of the art rejections depend on the application of either Little, standing alone or in combination with Chaum, McNair, or Schneier. As addressed in greater detail below, Little, Chaum, McNair, and Schneier do not support the Official Action's reading of them and the rejections based thereupon should be reconsidered and withdrawn. Further, the Applicant does

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

not acquiesce in the analysis of Little, Chaum, McNair, and Schneier made by the Official Action and respectfully traverses the Official Action's analysis underlying its rejections.

Claims 1, 5, and 10 were rejected under 35 U.S.C. §102(b) based on Little. Little describes a portable data module which generates both public and private encryption keys. In generating the encryption keys, random numbers are created and stored within a highly protected microcircuit wherein the circuitry is not accessible. Little, col. 4, lines 17-18. Little's random numbers are based on manipulations of a 32 byte storage structure called a random number seed accumulator (ACC). The ACC contents are segmented into segments which are then manipulated in various ways to randomize the ACC. The ACC is then the basis for each key created. See Little, page 14, line 16 et seq.

Referring to the protected circuitry contained within the portable electronic data module of Fig. 1 of Little, the one wire interface 15 connects to a host computer 10 for delivery of the generated keys. Figs. 2A-2C and 3 of Little illustrate the portable electronic data module in the form of a monolithic semiconductor chip. In these figures, the one wire interface is illustrated as a Universal Asynchronous Receiver/Transmitter (UART) which is used to communicate serially with a host computer. Little's portable data module addresses a secure device for providing encryption keys to a host computer based on a fixed 32 byte storage structure for the host computer's use and does not address a portable terminal comprising a display or an input for receiving financial data for a financial transaction.

In further contrast to Little, the present invention generates an encryption key based on one or more variable properties of the portable terminal to encrypt the financial data in the

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

portable terminal with the new key. To this end, the display of the portable terminal displays financial transaction options to a user. The user inputs financial data for the financial transaction. An encryption program is executed by the portable terminal to determine a new key based on one or more variable properties of the portable terminal. One example of such a variable property is the data stored in the dynamic heap of the memory of the portable terminal. Since the contents of the dynamic heap change based on the portable terminal's usage, each newly generated key will be unique. The portable terminal encrypts financial data associated with the financial transaction with the new key. Claim 1, as presently amended, reads as follows:

A portable terminal for encrypting information, the portable terminal comprising:
a display for displaying transaction options;
an input for receiving financial data for a financial transaction;
means for generating a new key for the financial transaction, wherein the new key is generated using one or more variable properties of the portable terminal; and
means for encrypting the financial data with the new key. (emphasis added)

Little does not disclose and does not make obvious "a display for displaying transaction options," as presently claimed in claim 1. Little does not disclose and does not make obvious "an input for receiving financial data for a financial transaction" as presently claimed. Little does not disclose and does not make obvious a "means for encrypting the financial data with the new key," as presently claimed in claim 1. Little simply discloses a secure device which generates encryption keys and requires electrical connection to a host for those keys to be utilized. Little's security is apparently based on a secure encryption circuit which is required to be sealed in a portable device. Claims 5 and 10 are similarly not anticipated and are not obvious from Little.

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

Further, Little does not disclose and does not make obvious a transaction system where a "portable terminal wirelessly transmitting encrypted information with the self service terminal," as presently claimed in claim 10.

Dependent claims 2 and 3 were rejected under 35 U.S.C. §103(a) based on Little and in view of various combinations of Chaum and McNair. Chaum and McNair fail to cure the deficiencies of Little. Since claims 2 and 3 depend from and contain all the limitations of claim 1 as presently amended, claims 2 and 3 distinguish from the references in the same manner as claim 1.

Claims 4, 6-9, and 11 were rejected under 35 U.S.C. 103(a) based on Little in view of Schneier. Schneier fails to cure the deficiencies of Little. Schneier is a textbook which describes various aspects of cryptography including encryption protocols. At page 63, Schneier describes the messaging protocol of Denning-Sacco where three users, Alice, Trent, and Bob, exchange messages between Alice and Trent so that Alice will eventually be able to communicate securely with Bob. Schneier teaches that after completing the protocol, Bob can masquerade as Alice. To address the potential of a masquerade by Bob, Schneier teaches adding the names identified as the intended communicants within the encrypted message. Schneier's high level description of the Denning-Sacco protocol does not address the limitations of the claims as presently amended.

Unlike Schneier and Little, certain of the claims of the present invention address the utilization of a challenge value to allow the receiver of an encrypted message such as a self service terminal to verify that the sender of an encrypted message can decrypt the messages, as well as, to verify secure communication can take place. Referring to page 9, line 15 – page 10,

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

line 8 and Fig. 5 of the present specification, the present invention describes how the challenge value and session key are originally created at the personal digital assistant (PDA) or portable terminal and communicated to a self service terminal such as an automated teller machine (ATM). The self service terminal decrypts the challenge value and conveys a new challenge value encrypted with the session key to the PDA. If the self service terminal has correctly responded to the original challenge, then the PDA responds to the self service terminal's challenge. Once the self service terminal verifies this response, secure communication may take place between the PDA and self service terminal.

Claim 8, for example, is directed to a method of communicating encrypted information between a portable terminal and a self-service terminal. Claim 8 recites "generating a challenge value based on the sequence of values; encrypting the new key and the challenge value using a public key; and transmitting the encrypted key and challenge value to the self-service terminal." (emphasis added)

Among its several failings, the high level description of an encryption protocol between Alice, Trent, and Bob as taught by Schneier does not teach and does not suggest the authentication between a portable terminal and a self service terminal as claimed. Schneier and Little, separately or in combination, do not teach and do not suggest "using one or more properties of the portable terminal to obtain a sequence of values" as claimed in claim 8. Schneier and Little, separately or in combination, do not teach and do not suggest "transmitting the encrypted key and challenge value to the self-service terminal" as claimed in claim 8. Further, Schneier does not provide a basis for modifying Little, and even if these items were

Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

modified to include some general, high level of encryption, the modified result would not meet the specifics of the presently amended claims.

The Official Action suggests that the DASS protocol on page 62 of Schneier teaches authentication with regard to claims 9 and 11. Although, in general, the DASS protocol may teach authentication, Schneier does not address the problem of authenticating communication between a portable terminal and a self-service terminal as claimed in claims 9 and 11.

Dependent claim 9 recites "awaiting a correct response to the transmitted challenge value being transmitted by the portable terminal before accepting any subsequent transaction at the self-service terminal." (emphasis added) Claim 11 is directed to determining if a self-service terminal is an authentic terminal. Claim 11 recites "transmitting the encrypted key and challenge to the self-service terminal; receiving a response from the self-service terminal, decrypting the response using the new key; and halting any further transmission unless the decrypted response includes a correct reply to the challenge value." (emphasis added)

Schneier and Little cannot simply be combined to obtain the presently claimed invention. By way of example, if the teachings of Schneier were combined into Little as the Official Action suggests, the problem of authenticating the secure communication between a portable terminal and a self service terminal would still exist.

The cited references do not appear to even recognize the problems addressed by the present invention. Further, the cited references do not teach or make obvious a structure which would solve the problems addressed by the present invention. The claims of the present invention are not taught, are not inherent, and are not obvious in light of the art relied upon.

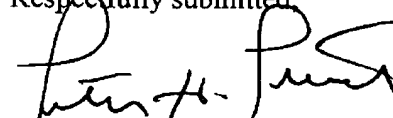
Appl. No. 09/651,979
Amdt. dated May 20, 2004
Reply to Office Action of February 26, 2004

New claims 12-20 have been added to cover certain aspects of the present invention. Independent claim 13 and claims 14-18 which depend on claim 13 address a portable terminal for encrypting information. These claims have additional limitations than claim 1 and at least define over the relied upon art in the same way as claim 1. Since dependent claims 12, 19, and 20 depend from and contain all the limitations of claims 1, 5, and 8, respectively, claims 12, 19, and 20 distinguish from the references in the same manner as claims 1, 5, and 8. Little, Chaum, McNair, and Schneier do not disclose and do not make obvious the portable terminal as claimed.

Conclusion

All of the presently pending claims, as amended, appearing to define over the applied references, withdrawal of the present rejection and prompt allowance are requested.

Respectfully submitted,



Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713-7736
(919) 806-1600